AO 106 (Rev. 04/10) Application for a Search Warrant

U.S. DISTRICT COURT
N.D. OF N.Y.
FILED
MAY 02 2017
LAWRENCE K. BAERMAN, CLERK
ALBANY

UNITED STATES DISTRICT COURT

for the

Northern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Silver-colored LG V20 Android smartphone in blue/silver case and Samsung Gear S2 Classic smartwatch, and attachments, located at U.S. Foods HR department

1:17-MJ-191-DJS

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

located in the Northern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2)(A) and (b)(1); 18 U.S.C. § 2252A (a)(5)(B) and (b)(2)	Receipt and distribution of, conspiracy to receive and distribute, and attempt to receive and distribute child pornography; possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography

The application is based on these facts:

See attached affidavit.

☑ Continued on the attached sheet.

☐ Delayed notice of ______ days (give exact ending date if more than 30 days: ____________) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

[signature]
Applicant's signature

Special Agent David C. Fallon
Printed name and title

Sworn to before me and signed in my presence.

[signature]
Judge's signature

Date: May 2, 2017

City and state: Albany, New York

Hon. Daniel J. Stewart
Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, David C. Fallon, having been first duly sworn, do hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant authorizing the search, seizure and examination of an LG V20 Android cellular smartphone, and a Samsung Gear S2 Classic smartwatch, and any attached storage devices, belonging to DAMIAN QUILLINAN, currently located in a locked file cabinet at the Human Resources department of the business U.S. Foods located at 755 Pierce Road in Clifton Park, New York.

2. I have probable cause to believe that contraband and evidence of a crime, fruits of a crime, and instrumentalities of violations of: 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of, conspiracy to receive and distribute, and attempt to receive and distribute child pornography); and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography), are located within the LG V20 Android cellular smartphone and Samsung Gear S2 Classic smartwatch, and any attached storage devices, as further described in Attachment A.

3. I am a Special Agent with Federal Bureau of Investigation (FBI) and have been assigned to the Albany Division, Albany, NY since May 1991. As such, I am an investigative or law enforcement officer of the United States within the meaning of Title 18 United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516(1). Prior to my employment as a Special Agent, I was a lawyer, licensed to practice in the State of Rhode

Island. As an FBI Special Agent, I am authorized to seek and execute federal arrest and search warrants for Title 18 criminal offenses, including offenses related to the sexual exploitation of minors, specifically 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of, conspiracy to receive and distribute, and attempt to receive and distribute child pornography); and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography). I have received extensive training and instruction in conducting online child sexual exploitation investigations. I have also been the affiant for and participated in the execution of numerous federal search warrants in child sexual exploitation investigations.

4. The statements contained in this affidavit are based in part on: my own investigation; information provided by FBI special agents and New York State Police ("NYSP") troopers; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents; information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by law enforcement computer forensic professionals; and my experience, training and background as a Special Agent (SA) with the FBI.

5. Because this affidavit is being submitted for the limited purpose of securing authorization for the requested search warrant, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish the necessary foundation for the requested warrant.

RELEVANT STATUTES

6. This investigation concerns alleged violations of: 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1),

Receipt, Transportation, and Distribution, and Conspiracy to Receive, Transport, and Distribute Child Pornography; and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2), Possession and Access, or Attempted Access with Intent to View Child Pornography.

a. 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) prohibits a person from knowingly receiving, distributing or conspiring to receive or distribute any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and

b. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

7. The following definitions apply to this Affidavit and attachments hereto:

a. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, legally obscene or that do not necessarily depict minors in sexually explicit conduct.

b. "Child Pornography," as used herein, is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

d. "Computer Server" or "Server," as used herein, is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system ("DNS") server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol ("IP") address so the computer hosting the web site may be located, and the DNS server provides this function.

e. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

f. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

h. "Computer passwords, pass-phrases and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

i. "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

j. "Host Name." A Host Name is a name assigned to a device connected to a computer network that is used to identify the device in various forms of electronic communication, such as communications over the Internet;

k. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

l. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

m. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line ("DSL") or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider ("ISP") over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

n. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

o. Media Access Control ("MAC") address. The equipment that connects a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter that is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

p. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

q. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

r. "Secure Shell" ("SSH"), as used herein, is a security protocol for logging into a remote server. SSH provides an encrypted session for transferring files and executing server programs.

s. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

t. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

u. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

v. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language ("HTML") and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP").

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

8. On July 29, 2016, the National Center for Missing and Exploited Children (NCMEC) received and forwarded to NYSP a cybertip from Synchronoss Technologies, Inc. ("Synchronoss") stating that on that same date possible child pornography had been uploaded to Verizon Wireless online "cloud" storage, which is administered by Synchronoss, from phone number (518) 888-5000. Specifically, nine images suspected to be child pornography were uploaded to the Verizon Wireless online "cloud" storage on July 29, 2016. NYSP troopers confirmed that the files appear to constitute child pornography. For example, one of the uploaded files entitled "8dcfae8753274dc395d46ae0feda3c7f_file2.jpg" depicts a prepubescent female between four and seven years-old lying on her stomach performing oral sex on an erect adult penis.

9. On September 12, 2016, NYSP troopers caused a subpoena to be issued to Cellco Partnership, dba Verizon Wireless requesting subscriber information, billing address, address or service, and connection records for the phone number 518-888-5000 from July 25, 2016 through August 29, 2016. The subpoena return revealed the sole individual associated with phone number 518-888-5000 to be DAMIAN QUILLINAN, 1422 Peaceable St., Ballston Spa, NY, with an alternate phone number of 518-788-4373. The account was activated on February 26, 2015 and was still active as of September 14, 2016. A search of public records furthered confirmed that the above-referenced phone number and address were associated with QUILLINAN.

10. On September 30, 2016, myself and NYSP troopers assigned to Troop G, CCU, and the ICAC task force executed a search warrant issued by the Honorable Vernon L. Ketchum, Town Justice for Saratoga County, Town of Charlton Criminal Court at 1422 Peaceable Street, Ballston Spa, New York. The search warrant was obtained on September 28, 2016, based on the above information.

11. Your affiant was present at the above address when the search warrant was executed. Pursuant to the search warrant, law enforcement officers recovered various electronic devices from QUILLINAN's bedroom that, based on forensic previews, were determined to contain child pornography, including but not limited to, one (1) gray Samsung Galaxy S7 Edge cell phone, one (1) homemade desktop computer, one (1) black Digital Storm laptop computer, one (1) black Asus tablet, three (3) external hard drives, two (2) thumb drives, and several DVDs.

12. During a forensic preview of the homemade desktop computer, which contained a 2GB Hitachi hard drive labeled "Made in China," located in QUILLINAN's bedroom, agents located

approximately 51 video files and 13,000 image files that appear to constitute child pornography. Two of these files are described as follows:

(a) A 10.6 MB video file entitled "'video180.vid_bogdan_9yo_.avi'" which depicts a nude male child approximately nine years-old being forced to perform oral sex on an erect adult penis and inserting a foreign object anally. This file was located in a folder on the computer's desktop.

(b) A 9.7 MB video file entitled "video156.russian_kids_-_7_yo_and_9_yo_play_with_man_cock_suck_02.avi" which depicts a female child between the ages of seven and nine performing oral sex on an erect adult penis. This file was located in the computer's downloads folder.

13. During a forensic preview of a 500 GB black Seagate external hard drive labeled "Product of China," located in QUILLINAN's bedroom, agents located approximately 179 video files and 100 image files that appear to constitute child pornography." Two of these files are described as follows:

(a) A 17.2 MB video file entitled "XXX - Incent - 5yo raped_ hymen penetrated - kiddy little girl young porn real child sex baby pedo (no sound).mpg" which depicts a nude female child approximately five years-old being vaginally penetrated by an erect adult penis. This file was located in a folder entitled "limewire."

(b) A 10.3 MB video file entitled "babyfucker_Venezuela-girls(3-4yo)-2.avi" which depicts two female children between the ages of 3 and four years-old performing oral sex on an erect adult penis, and being anally and vaginally penetrated by an erect adult penis. This file was located in a sub-folder entitled "mov" in a folder entitled "stuff."

14. During the execution of the search warrant, NYSP troopers interviewed QUILLINAN who was present at the residence at the time of the execution of the warrant. QUILLINAN admitted to using the Internet on his homemade desktop computer to search for, view, and download images and videos of child pornography, which he saved to various external electronic devices during the prior five years. QUILLINAN further admitted that he knew it was illegal to possess the images and videos depicting child pornography, but that it had become an addiction for him. QUILLINAN further admitted that he had also used his Samsung Galaxy S7 Edge smartphone to access and download child pornography.

15. Following his arrest and arraignment on state child pornography charges, QUILLINAN was released on bond. QUILLINAN continued working at U.S. Foods located at the SUBJECT PREMISES. On March 28, 2017, QUILLINAN was arrested at his office located at the SUBJECT PREMISES on a federal arrest warrant issued in case 17-MJ-121 (DJS). According to U.S. Foods Human Resource officer Rae Weaver, a silver-colored LG V20 Android cellular smartphone in a blue/silver case, and a Samsung Gear S2 Classic smartwatch, both belonging to QUILLINAN, were recovered in his office after the arrest. The smartphone and smartwatch were retrieved by Ms. Weaver and placed in a locked cabinet in the U.S. Foods Human Resources department office located at 755 Pierce Road in Clifton Park, New York, where they reside as of May 2, 2017.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

16. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

17. Child pornographers can now transfer printed photographs into a computer-readable format

with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

18. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

19. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options

available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person.

20. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

21. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

22. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a

computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

23. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices (like hard drives, SD cards, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

24. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit ("CPU"). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

25. Based upon my training and experience and conversations with other law enforcement personnel, I am aware that smartphones and smartwatches, such as the LG V20 Android and Samsung Gear S2 Classic, and any attached storage devices, function as computers and run off software similar to that of computer systems. Of note, smartphones and smartwatches have the ability to access the Internet by connecting to existing wi-fi networks or through a cellular data subscription, and are capable of storing vast amounts of images using their internal storage, which can be expanded with additional SD cards. I am aware that the LG V20 Android smartphone contains 64GB of memory, which can be expanded with a microSD card for an additional 2TB of storage. I am further aware that the Samsung Gear S2 Classic smartwatch runs on Android software,

can be linked to other Android devices including smartphones, and contains between 512MB and 4GB of memory, depending on the model.

26. Furthermore, because there is probable cause to believe that the LG V20 Android smartphone and Samsung Gear S2 Classic smartwatch, and any attached storage devices, are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED REGARDING ELECTRONIC DATA

27. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. on-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims, and a scan for encryption software;

b. on-site forensic imaging of any computers that may be partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for examination; such imaging may require several hours to complete and require law enforcement agents to secure the search scene until that imaging can be completed;

c. examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

d. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

e. surveying various file directories and the individual files they contain;

f. opening files in order to determine their contents;

g. scanning storage areas;

h. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and

i. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

CONCLUSION

28. Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause to believe that QUILLINAN, has committed offenses in violation of 18 U.S.C. § 2252A, and there is probable cause to believe that evidence of violations of 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of, conspiracy to receive and distribute, and attempt to receive and distribute child pornography); and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography), is within the LG V20 Android cellular smartphone and Samsung Gear S2 Classic

smartwatch, and any attached storage devices, belonging to DAMIAN QUILLINAN, currently located in a locked file cabinet at the Human Resources department of the business U.S. Foods located at 755 Pierce Road in Clifton Park, New York.

Special Agent David C. Fallon
Federal Bureau of Investigation

Sworn to me this day of May, 2017

Hon. Daniel J. Strewart
United States Magistrate Judge

ATTACHMENT A

PROPERTY TO BE SEARCHED

The property to be searched is a silver-colored LG V20 Android cellular smartphone in a blue/silver case and a Samsung Gear S2 Classic smartwatch, and any attached storage devices, belonging to DAMIAN QUILLINAN, located in a locked file cabinet at the Human Resources department of the business U.S. Foods located at 755 Pierce Road in Clifton Park, New York.

This warrant authorizes the forensic examination of the above device for the purpose of identifying the electronically stored information described in Attachment B

ATTACHMENT B

ITEMS TO BE SEARCHED FOR AND SEIZED

Items of evidence of violations of 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of, conspiracy to receive and distribute, and attempt to receive and distribute child pornography); and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography):

Computers and Electronic Data

1. The authorization includes the search of electronic data within the property identified in Attachment A to include deleted data, remnant data and slack space. The seizure and search of the property identified in Attachment A will be conducted in accordance with the affidavit submitted in support of this warrant.

2. Computer hardware, meaning any and all computer equipment, including any electronic storing devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer hardware is any data processing hardware (such as central processing units and self-contained laptop or notebook computers); internal and peripheral storage devices (such as thumb drives, flash drives, SD (secure digital) cards, fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical and compact storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections, recording equipment, RAM and ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing, or signaling devices, and electronic tone generating devices); and any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).

3. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems, software, application software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

4. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

5. Computer passwords and data security devices, meaning any devices, programs, or data, whether themselves in the nature of hardware or software, that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer related documentation, or electronic data records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips and circuit boards); passwords; data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data, or to otherwise render programs or data into usable form.

6. Any computer or electronic records, documents and materials referencing or relating to the above described offenses. Such records, documents or materials, as well as their drafts or modifications, may have been created or stored in various formats, including, but not limited to, any hand-made form (such as writing or marking with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negatives, video tapes, motion pictures, or photocopies); any mechanical form (such as photographic records, printing or typing); any electrical, electronic or magnetic form (such as tape recordings, cassettes, compact disks); or any information on any electronic or magnetic storage device (such as thumb drives, flash drives, sd (secure digital) cards, floppy diskettes, hard disks, CD-ROMs, DVDs, optical disks, printer buffers, soft cards, memory calculators, electronic dialers, or electronic notebooks), as well as printouts or readouts from any magnetic storage device.

7. Any electronic information or data, stored in any form, which has been used or prepared for use either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), or any computer or computer system. The form that such information might take includes, but is not limited to, thumb drives, flash drives, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, CD-ROM disks, DVDs, video cassettes, and other media capable of storing magnetic or optical coding.

8. Any electronic storage device capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and using electronic data used to conduct computer or Internet-based communications, or which contains material or data, obtained through computer or Internet-based communications, including data in the form of electronic records, documents and materials, including those used to facilitate interstate communications, included but not limited to telephone (including mobile telephone) and Internet Service Providers. Included within this paragraph is any

information stored in the form of electronic, magnetic, optical, or other coding, on computer media, or on media capable of being read by a computer or computer-related equipment, such as thumb drives, flash drives, SD (secure digital) cards, fixed disks, external hard disks, removable hard disk cartridges, CDs, DVDs, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, laser disks, or other memory storage devices.

Documents, Records and Evidence

9. Records of personal and business activities relating to the operation and ownership of the property identified in Attachment A.

10. Any records or documents pertaining to accounts held with Internet Service Providers or of Internet use.

11. Records of address or identifying information for QUILLINAN and any personal or business contacts or associates of his, (however and wherever written, stored or maintained), including contact lists, buddy lists, email lists, ICQ addresses, IRC names (a.k.a., "Nics"), user ID's, eID's (electronic ID numbers) and passwords.

12. Evidence indicating how and when the property identified in Attachment A were accessed or used to determine the chronological context of access, use, and events relating to the crimes under investigation and to user.

13. Evidence of the attachment to the property identified in Attachment A of other storage devices or similar containers for electronic evidence.

14. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from electronic media.

15. Evidence of the times any of the property identified in Attachment A was used.

16. Passwords, encryption keys, and other access devices that may be necessary to access any the property identified in Attachment A.

17. Documentation and manuals that may be necessary to access or to conduct a forensic examination of the property identified in Attachment A.

18. Records of or information about Internet Protocol addresses used by the property identified in

Attachment A, as well as records of or information about the property's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

19. Contextual information necessary to understand the evidence described in this attachment.

Materials Relating to Child Erotica and Depictions of Minors

20. Any and all visual depictions of minors, including, but not limited to, sexually explicit images of minors.

21. Any and all chats, chat logs, emails, and other text documents, describing or relating to sexually explicit conduct with children, as well as fantasy writings regarding, describing, or showing a sexual interest in children.

22. Any and all address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18 United States Code, § 2256(2).

23. Any and all notebooks and any other records reflecting personal contact, and any other activities, with minors who may be visually depicted while engaged in sexually explicit conduct, or engaged in sexually explicit chat, email, or other communications.

24. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, notes, and sexual aids.